Darin M. Sands, *SandsD@LanePowell.com*
LANE POWELL PC
601 SW Second Ave, Suite 2100
Portland, OR 97204-3158
Telephone: 503.778.2117

Daniel R. Warren, *dwarren@bakerlaw.com*
David A. Carney, *dcarney@bakerlaw.com*
BAKER & HOSTETLER LLP
127 Public Square, Suite 2000
Cleveland, OH 44114
Telephone: 216.621.0200

Paul G. Karlsgodt, *pkarlsgodt@bakerlaw.com*
BAKER & HOSTETLER LLP
1801 California Street, Suite 4400
Denver, CO 80202
Telephone: 303.861.0600

James A. Sherer, *jsherer@bakerlaw.com*
BAKER & HOSTETLER LLP
45 Rockefeller Plaza
New York, NY 10111
Telephone: 212.589.4200

Attorneys for Defendant Premera Blue Cross

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

IN RE: PREMERA BLUE CROSS CUSTOMER DATA SECURITY BREACH LITIGATION

This document relates to all actions.

Case No. 3:15-md-2633-SI

PREMERA'S OPPOSITION TO PLAINTIFFS' MOTION FOR SANCTIONS FOR DISCOVERY MISCONDUCT[*]

FILED UNDER SEAL

[*] LR 26-3 Certification: Defendant certifies that this opposition memorandum does not exceed the word-count limitation agreed to in the Joint Motion to Extend Word-Count Limitation for Plaintiffs' Motion for Sanctions.

Introduction

Premera took reasonable steps to preserve evidence and has committed no discovery "misconduct." To the extent that information Plaintiffs have requested was lost either on the device ("A23567-D") or within the Vontu data loss prevention ("DLP") logs, such information was accidentally lost. Other facts in the record clarify that neither A23567-D nor DLP logs contained critical information about the attackers' activities or the question of whether they removed information from Premera's network. If there is any prejudice caused to Plaintiffs by not having access to these two items it is minimal, and the sanctions requested by Plaintiffs are unwarranted. Pursuant to the applicable standard in Fed. Rule Civ. P. 37(e), the Court should deny the relief requested in Plaintiffs' Motion.

Applicable Legal Standard – Rule 37(e)

Plaintiffs rely on the Court's inherent, discretionary right to sanction, asking the Court to order sanctions of an adverse jury instruction at trial, an order preventing expert testimony, and an order excluding evidence. However, Plaintiffs have not addressed the limits to the Court's inherent discretionary power to sanction imposed by Rule 37(e) as amended in 2015. The Rules Committee specifically "sought to foreclose 'reliance on inherent authority or state law to determine when certain [curative or sanctioning] measures should be used,'"[1] and courts considering the applicable legal standard have adopted this reasoning.[2]

The sanctions requested in Plaintiffs' Motion are properly governed by amended Rule 37(e). Under Rule 37(e), failure to preserve electronically stored information ("ESI") is sanctionable only if all of the following "Initial Criteria" are true:

1. ESI has been lost;
2. The lost ESI should have been preserved in anticipation of litigation;
3. That loss is the result of the responding party's failure to take reasonable steps to preserve the ESI; *and*
4. The ESI cannot be restored or replaced through additional discovery.

The Rule 37(e) standard is additive; in order for the Court to consider any measures under Rule 37(e)(1) or Rule 37(e)(2), all of the Initial Criteria must be met. Even if ESI is lost, relief under Rule 37(e) requires the remainder of the Initial Criteria to be met as well.[3]

If all of the Rule 37(e) Initial Criteria have been met, Rule 37(e)(1) then requires

[1] According the 2015 Rules Committee Notes, amended Rule 37(e) "authorizes and specifies measures a court may employ if information that should have been preserved is lost, and specified the findings necessary to justify these measures. It therefore forecloses reliance on inherent authority or state law to determine when certain measures should be used." Fed. R. Civ. P. 37(e).

[2] *Matthew Enter., Inc. v. Chrysler Group LLC*, 2016 WL 2957133, at *1 (N.D. Cal. May 23, 2016*); see also Fiteq Inc. v. Venture Corp.*, 2016 WL 1701794, at *3 (N.D. Cal. Apr. 28, 2016), *Snider v. Danfoss, LLC*, 2017 WL 2973464, at *3 (N.D. Ill. July 12, 2017) ("After December 1, 2015, Rule 37(e) provides the specific – *and sole* – basis to sanction a party for failing to preserve" ESI.) (emphasis added).

[3] *Konica Minolta Bus. Solutions v. Lowery Corp.*, 2016 WL 4537847, at *6 (E.D. Mich. Aug. 31, 2016) ("[the moving party] is not entitled to relief under 37(e), even if it is shown the ESI was lost").

the Court to determine whether the lost ESI—here, data on A23567-D or in the DLP logs—has prejudiced Plaintiffs. If no prejudice occurred, sanctions are unwarranted. If the Court determines Plaintiffs have been prejudiced by the loss of the ESI, then "measures no greater than necessary to cure the prejudice" may be ordered.[4] In order to levy the severe sanctions available only under Rule 37(e)(2), Premera must have acted with the specific intent to deprive Plaintiffs of the use of lost ESI, which Premera categorically has not.

In sum, if the Court determines the answer to any of the Initial Criteria is "no," Premera cannot be sanctioned under Rule 37(e). Even when the Initial Criteria are met, the Court may sanction under Rule 37(e) only if Plaintiffs have been prejudiced by the lost ESI, or if the loss of the ESI was the result of a specific intent to deprive Plaintiffs of its use.

While Plaintiffs are correct that the ESI at issue in their Motion is unavailable as requested, the other Rule 37(e) Initial Criteria required for sanctions have not been met. The loss of the ESI was due to inadvertent errors in both instances (an accidentally recycled device and the loss of log data during a critical system upgrade), as Premera explained to Plaintiffs. These are *not* failures by Premera to take reasonable steps to preserve ESI. Concerning the DLP logs, it is questionable that any responsive ESI existed to preserve.

Even assuming the Initial Criteria of Rule 37(e) are met, the lost ESI is still not sanctionable. Plaintiffs' requested sanctions are aimed at shoring up their argument of

[4] Fed. R. Civ. P. 37(e)(1).

exfiltration, but nothing in the missing ESI would have demonstrated exfiltration, especially as pertains to the .RAR files that Plaintiffs inexplicably cite in their Motion as connected to the lost DLP logs and A23567-D. The ESI at issue is unlikely to be relevant to Plaintiffs' claims; its loss is minimally prejudicial. Here, additional discovery may mitigate the lost ESI, and other discovery already in Plaintiffs' possession addresses certain of their concerns. Plaintiffs' requested sanctions are therefore greater than necessary to cure any prejudice caused by the spoliated evidence.[5]

Amended Rule 37(e)(2) requires an intent to deprive for the imposition of more severe sanctions, including adverse inferences. This is a higher standard than the willfulness standard Plaintiffs present in their Motion. Willfulness requires intentionality, but the intent to deprive requires *purposeful* intentionality. Premera did not act with any intent to deprive Plaintiffs of the use of ESI in this litigation, and Plaintiffs' requested sanctions are foreclosed by Rule 37(e).

A23567-D and the DLP Logs are ESI and Properly in the Scope of Rule 37(e)

Plaintiffs' Motion identifies the spoliated evidence as part of two categories of discovery: "(1) files contained on the hard drives of computers compromised by the hackers; and (2) log files from Premera's various types of data security software."[6] The 2006 Committee notes to Rule 34 define ESI as "information that is stored in a medium from which it can be retrieved and examined" and advise that the definition is expansive and applicable to other Rules into which the term ESI is inserted.[7] This definition

[5] *Id.*
[6] ECF No. 182 at 3.
[7] Fed. R. Civ. P. 34.

encompasses A23567-D and the DLP logs.

Discussion of Device A23567-D

A23567-D was one of 35 devices identified and examined by Mandiant in its investigation;[8] the remaining 34 have been preserved and inspected by Plaintiffs.[9] Specifically, A23567-D was a Premera desktop machine assigned to employee Troy Rampy at the time of the cyberattack.[10] The "D" in the naming convention designates this as a machine with a Microsoft Developer Network ("MSDN") license, which provides user access to Microsoft products for development and testing. While Plaintiffs claim that developer machines were automatically "afforded security clearance to Premera's most sensitive databases,"[11] A23567-D only provided increased functionality for the Microsoft programs Mr. Rampy was tasked with developing. MSDN did not otherwise expand his user access to Premera's network.[12]

Premera attempted to preserve A23567-D along with the other Mandiant-identified devices, issuing a ticket for its collection on March 2, 2015.[13] Due to a labelling error, A23567-D was inadvertently sent to a staging area in Premera's Client

[8] Declaration of Jason T. Dennett ("Dennett Decl.") Ex. 3, February 5, 2015 Mandiant Status Report from Mr. Foscue to Mr. Gowan, at 1, 5 (PBC_TAR00845898, PBC_TAR00845902); Ex. 5, February 3, 2015 Mandiant Status Report from Mr. Foscue to Mr. Gowan, at 1 (PBC00264273).

[9] Dennett Decl. Ex. 1, June 26, 2015 Mandiant Intrusion Investigation Report ("Mandiant Report"), at 49 (PBC00023992).

[10] *See* Dennett Decl. Ex. 7, Premera's Response to Plaintiffs' Interrogatory 14 for additional detail.

[11] ECF No. 182 at 5.

[12] Declaration of Joel Seymour at ¶¶ 2-3; *see also* Declaration of James A. Sherer ("Sherer Decl.") Ex. 1, Deposition of William Gowan ("Gowan Dep.") at 170:10-20.

[13] Sherer Decl. Ex. 2, COSMOS Ticket Spreadsheet (PBC00262488, line 2052).

Technology Services location, subsequently sent to Premera's Personal Computer Distribution Center on September 29, 2016, and listed as destroyed on December 16, 2016. A23567-D was the only Mandiant-identified device that was not preserved by Premera's collection and preservation procedures.

Rule 37(e) Initial Criteria No. 1: Whether A23567-D ESI Was Lost

Because of its accidental destruction, Premera is unable to provide Plaintiffs with direct access to ESI from A23567-D. However, it is unlikely that A23567-D contained ESI that Plaintiffs require for proof of their contentions. Numerous contemporaneous forensic experts, including those at Mandiant, CrowdStrike, and the Federal Bureau of Investigation, analyzed A23567-D with the opportunity to capture forensic images for further evaluation. They captured none, because A23567-D was not important for their forensic investigations of the cyberattack, Premera's remediation efforts, or Premera's further security efforts.[14] Plaintiffs' Expert, Matthew Strebe, had the opportunity to review forensic images of 34 of the 35 devices and stated that he did not find "anything beyond that that was reported by Mandiant."[15] This suggests it is unlikely Plaintiffs would find anything unreported by Mandiant on A23567-D if Plaintiffs could examine it.

Plaintiffs' discovery conduct supports the relative unimportance of the ESI from A23567-D. According to Plaintiffs, one of the key ways to look for evidence of

[14] Sherer Decl. Ex. 3, Deposition of John Twitchell ("Twitchell Dep.") at 256:18-21 ("Q. "Do you recall it being significant that PHOTO malware was found on that [A23567-D] system?" A. "Not especially, no."). *See also id*. at 168:23-170:23 for discussion of the functionality of PHOTO malware and its limitations compared to SOGU, and Ex. 4, Mandiant 30(b)(6) Deposition of Daniel Paul Hranj ("Mandiant 30(b)(6) Dep.") at 154:16-23 and 155:3-19 for discussion of Mandiant's analysis of PHOTO malware.

[15] Sherer Decl. Ex. 5, Deposition of Matthew Strebe ("Strebe Dep.") at 143:23-25.

exfiltration is to examine files left behind, which requires either the computer's original hard drive or a copy of all data on that drive for a forensic expert to review.[16] Premera produced a copy of the Mandiant Intrusion Investigation Report in early 2016. Despite receiving the Report, Plaintiffs demonstrated no specific interest in A23567-D until they became aware that the computer was missing in early 2018, demonstrating the nonessential role of this ESI as part of discovery in this case.[17]

Plaintiffs now assert that their inability to "conduct the same type of forensic examination done by Mandiant to test Mandiant's opinions on which Premera intends to rely" unfairly prejudices them, but based on the scope of Plaintiffs' Request for Inspection, conducting a full forensic examination was never their goal.[18] Regardless, Mandiant's opinions related to any potential exfiltration rely on their analysis of evidence of seven .RAR files found during their investigation of servers that Plaintiffs' expert did examine: MLTPBTSV6J and MLTPBMX5A. None of the forensic experts identified .RAR files on A23567-D or any other remnants that would have supported exfiltration via this device. Moreover, Premera does not rely on the opinions of Mandiant but on

[16] ECF No. 182 at 3, citing Declaration of Matthew Strebe ("Strebe Decl.") ECF No. 166, ¶¶ 73-79; 225-229.

[17] Plaintiffs write that they sought "evidence that was left behind on the 35 computers the hackers compromised" (ECF No. 182 at 3), and "requested an image of A23567-D for purposes of conducting their own forensic investigation of the hacker activity." (ECF No. 182 at 5.) Plaintiffs further allege they "served a request for inspection on Premera asking for forensic images of all 35 of the affected computers." (ECF No. 182 at 4.) However, Plaintiffs' Request for Inspection only asked for "an imaged copy of all server backups," (Dennett Decl. Ex. 2 at 1) to be made of servers in place at Premera at the time of imaging, not those in the Mandiant Report, and seemingly not for the purpose of recreating Mandiant's forensic analysis or that completed by CrowdStrike or the FBI.

[18] ECF No. 182 at 5.

reasonable inferences drawn from the facts that Mandiant reported after its investigation. These same facts have been made available to Plaintiffs through Mandiant's updates, recommendations, and reports.

Rule 37(e) Initial Criteria No. 2: Whether Lost ESI From A23567-D Should Have Been Preserved

Premera unsuccessfully attempted to preserve ESI associated with A23567-D. Premera's documentation for A23567-D[19] demonstrates that, like other ESI preserved during Premera's remediation following the cyberattack, Premera intended to remove A23567-D, replace it, and preserve it with other Premera evidence.

Rule 37(e) Initial Criteria No. 3: Whether Loss of A23567-D ESI Was the Result of Premera's Failure to Take Reasonable Steps to Preserve

As described above, Premera took reasonable steps to preserve A23567-D. Premera put A23567-D under legal hold, collected it for preservation, but lost track of it during a chaotic weekend where Premera sought to take its IT systems offline to eradicate the intruder from its network and implement remediation efforts. Premera accidentally sent A23567-D to the wrong location, which inadvertently put A23567-D into its normal process for retiring computer equipment instead of preserving it. The fact that Premera did not successfully preserve A23567-D cannot meet the subjective reasonability standard of Rule 37(e), or the standard would be met every time ESI went missing in any

[19] *See* Sherer Decl. Ex. 2, COSMOS Ticket Spreadsheet (PBC00262488, line 2052).

matter.[20]

Rule 37(e) Initial Criteria No. 4: Whether ESI from A23567-D Can be Restored or Replaced through Additional Discovery

The missing ESI on A23567-D is not critical to Plaintiffs' proof in this matter. Moreover, Mandiant contemporaneously examined A23567-D,[21] and Plaintiffs may use the results of that analysis for any admissible purpose. Notably, Mandiant's analysis of the device would be admissible notwithstanding the best evidence rule, since the device is no longer available. Plaintiffs have provided no reason to conclude that Mandiant's analysis was not at least as comprehensive and complete as any independent work they would have conducted.[22] Plaintiffs may also rely on CrowdStrike's investigation and report provided to Plaintiffs, as CrowdStrike also analyzed A23567-D.[23]

[20] Minutes, Standing Committee Meeting, May 29-30, 2014 at 6 (quoting Judge David Campbell, Chair of the Rules Committee, to the effect that Rule 37(e) is not "a strict liability rule that would automatically impose serious sanctions if information is lost").

[21] Sherer Decl. Ex. 6, 30(b)(6) Deposition of Joel Seymour from Sept. 21, 2017 at 52:10-19 and Ex. 3, Twitchell Dep. at 263:13-19.

[22] Plaintiffs' Motion claims Mandiant's investigation reached conflicting conclusions, but this is not true. As demonstrated by Dennett Decl. Ex. 3, the February 5, 2015 Mandiant Status Report, Mandiant initially noted that the .RAR files could indicate data staging and theft. Dennett Decl. Ex. 4, the March 3, 2015 Mandiant Status Report states Mr. Foscue thought it more likely than not that the files were created by the attacker. The Mandiant Report at 49 explains no determination was made about the nature or contents of the .RAR files or who created them. This final statement does not conflict with the prior statements, none of which are definitive.

[23] Sherer Decl. Ex. 7, CrowdStrike's Project: Blue Oxford Final Report at 23 (PBC00169161) (Appendix of the list of hostnames of systems CrowdStrike examined with FFC during their assessment).

ESI From A23567-D Does Not Meet the Criteria for Sanctions Under Rule 37(e)

Premera did not fail to take reasonable steps to preserve A23567-D. Instead, it employed the same process for A23567-D as it did for every other preserved Mandiant-identified device. Further, additional evidence adequately analyzes A23567-D in a manner in keeping with Plaintiffs' intended use of this ESI. Plaintiffs' unsupported conjecture that A23567-D would have been the perfect device from which intruders could have "staged" exfiltration of data does nothing to negate the other expert work performed, which found no evidence of this. In fact, forensic experts who examined A23567-D identified a different device as the likely staging computer: MLTPBTSV6J, a server containing the .RAR file remnants Plaintiffs focus on.[24]

Finally, even if the Court finds that lost ESI from A23567-D meets all of the Rule 37(e) Initial Criteria, Plaintiffs have failed to show prejudice from the missing ESI or that Premera acted with the specific intent to deprive them of ESI from A23567-D as required for sanctions.

Discussion of the DLP Logs

At the time of the cyberattack, Premera used Vontu DLP Version 11.6,[25] which maintained 365 days of user-defined logs in an Oracle database. During a required Vontu DLP system upgrade in the summer of 2015,[26] an accidental, catastrophic error occurred where the prior year's DLP logs were lost and not recoverable from the server or back-up

[24] Dennett Decl. Ex. 8, Excel Spreadsheet Provided by non-party FireEye, Inc. in this litigation (FIREEYE0000001, at p. 24 of 96). No .RAR files were identified by any experts on A23567-D despite specifically looking for exactly this type of file.

[25] Declaration of Edwin Christian ("Christian Decl.") at ¶ 11.

[26] Christian Decl. at ¶¶ 10-11.

tapes after the transfer to the upgraded DLP system.[27]

Plaintiffs assert that these logs "contain critical evidence necessary for a full assessment of the hacker's activity."[28] Plaintiffs' also observe correctly that Vontu DLP "can be programmed to alert" and log if sensitive information exits the network.[29] Such logs would only assist Plaintiffs' aims, however, if Vontu was specifically programmed to observe and alert for this type of cyberattack activity.[30] It was not. While Plaintiffs' Expert had limited Vontu experience,[31] he agreed that Premera "did not have their various security proxies properly configured to detect the flow of [sensitive information]."[32] Premera's fact witnesses also noted contemporaneous issues with the configuration of Vontu that would have limited its logging capabilities.[33]

The lost DLP logs were very limited in scope and would not have addressed Plaintiffs' claims of .RAR file exfiltration for two reasons. First, Vontu's detection of protected personal information generated alerts. Vontu sent each alert, supplementing any DLP logs, to Premera's Vontu Alert mailbox for evaluation and escalation, but only if Vontu detected protected personal information not subject to exceptions.

[27] *Id*. at ¶¶ 12-14. See also Sherer Decl. Ex. 3, Twitchell Dep. at 230:12-232:1 regarding the scope and potential business impact of this needed upgrade.
[28] ECF No. 182 at 7.
[29] *Id.*
[30] Christian Decl. at ¶¶ 3-9.
[31] Sherer Decl. Ex. 5, Strebe Dep. at 191:24-25 ("Q. How about Vontu? A. I've heard of Vontu. I've never used it.").
[32] *Id.* at 159:1-10.
[33] Sherer Decl. Ex. 8, Deposition of Eric Robinson ("Robinson Dep.") at 114:10-23 and 116:13-17; Ex. 9, Deposition of Jerry Vergeront at 95:1-7 and 129:7-25; Ex. 10, Deposition of Edwin Christian at 187:23-190:8; Ex. 1, Gowan Dep. at 20:4-24:23, 140:1-141:10, and 165:6-17.

Second, certain compressed files, such as .RAR or .TAR files, were invisible to Vontu as configured during the cyberattack; therefore, movement of these files through Premera's network would have produced no alerts or log entries.[34] For these reasons, the absence of DLP logs does not critically impact Plaintiffs' assessment of this matter's evidence.

Rule 37(e) Initial Criteria No. 1: Whether Relevant DLP Logs Were Lost

Premera cannot provide Plaintiffs with access to ESI from DLP log data lost during the upgrade. However, the DLP logs likely contained no ESI required for any proof in this matter because of the limited Vontu logging during the relevant time period.[35] Also, Premera has already provided Plaintiffs a forensic image of MLTPSAP185, one of Premera's Vontu application servers[36] identified by Mandiant as one of the 35 compromised systems.[37] While Plaintiffs' Expert has had access to that image for months, he did not "specifically search for the files that contained logs on [the images]…[b]ecause it was not an answer to one of the questions [he] had when [he] was looking at those machines at that time."[38] Premera has also produced Vontu Alert emails to Plaintiffs and is willing to produce additional Vontu Alert email to Plaintiffs if so

[34] Christian Decl. at ¶ 9. *See also* Sherer Decl. Ex. 8, Robinson Dep. at 116:13-17 discussing the fact that personally identifiable information could be transferred to certain email accounts without Vontu's detection.

[35] *Id.* at ¶¶15-16.

[36] *See* Sherer Decl. Ex. 11 (PBC00041324, "Compromised" Tab, Row 27) and Ex. 12 (PBC_TAR00127396).

[37] Dennett Decl. Ex. 1, June 26, 2015 Mandiant Report, at 49 (PBC00023992).

[38] Sherer Decl. Ex. 5, Strebe Dep. at 242:22-243:5.

ordered.[39]

Rule 37(e) Initial Criteria No. 2: Whether Premera Was Required to Preserve ESI from DLP

There was no DLP log data that Premera was required to preserve that would be relevant to the claims in this matter due to the limited logging Vontu was performing at the time of the cyberattack.

Rule 37(e) Initial Criteria No. 3: Whether Loss of DLP ESI Was the Result of Premera's Failure to Take Reasonable Steps to Preserve

Premera's actions were not unreasonable given the then-current operation of Vontu, the required mid-2015 system upgrade, and Premera's unsuccessful attempts to capture and transfer the DLP logs from the prior Vontu instance.

Rule 37(e) Initial Criteria No. 4: Whether DLP Log Data Can be Restored or Replaced Through Additional Discovery

Plaintiffs claim that "no other source of data will show what a DLP log would: hackers transferring customers' personal information out of Premera's network."[40] Plaintiffs also state that this exfiltration happened through the use of .RAR files.[41] But lost DLP logs would have no .RAR file information due to Vontu's contemporaneous configuration during the cyberattack; therefore there is no missing .RAR file or related

[39] *See*, *e.g.*, Sherer Decl. Ex. 13 (PBC_TAR00125305) and Ex. 14 (PBC_TAR00525162).
[40] ECF No. 182 at 8.
[41] *Id.* at 4-5.

exfiltration DLP log data.[42] If there was DLP log data related to attempted violations of Premera's DLP business rules regarding exfiltration of personal information (through email or device copying), such violations would have generated both DLP log data and alerts sent to the Vontu Alert mailbox. If Plaintiffs wish to recreate logs of DLP policy violation data, they may be able to through Vontu Alert email.

ESI From DLP Logs Does Not Meet the Criteria for Sanctions Under Rule 37(e)

Plaintiffs cannot prove Initial Criteria No. 1 – that Premera lost relevant DLP Logs, because there was never any truly *relevant* DLP log data. Similarly, Plaintiffs cannot prove Initial Criteria No. 2 because it is unlikely that specific DLP data should have been preserved related to this litigation. Initial Criteria No. 3 fails as Premera's actions when upgrading Vontu were reasonable, and Initial Criteria No. 4 is inapplicable as any arguably relevant data also likely exists on the MLTPSAP185 Vontu device produced to Plaintiffs, in automated alerts already produced to Plaintiffs, or in Vontu Alert email that Premera will collect and produce if so ordered by the Court.

Even if the Court finds that the lost ESI from the DLP logs meets all of the Rule 37(e) Initial Criteria, Plaintiffs have not met the Rule 37(e) Criteria for Sanctions, as Plaintiffs have not demonstrated either prejudice from the missing ESI or that Premera acted with the specific intent to deprive Plaintiffs of ESI from the DLP logs.

[42] Christian Decl. at ¶ 9.

Sanctions are Unwarranted

Premera took reasonable steps to preserve the ESI; therefore, no sanctions are warranted under Rule 37(e). Even if Premera *had* failed to take reasonable steps to preserve the ESI, the sanctions should be limited to curing any minimal prejudice caused by such loss.

Plaintiffs allege that "harm was done to every member of the Class when their sensitive information was exposed to an unauthorized third party,"[43] and argue that proving exfiltration is required for this argument. But, Premera has not denied the possibility that attackers had access to the information. Premera's cybersecurity notification letters state: "[o]ur investigation determined that the attackers *may have* gained unauthorized access to your [sensitive] information... The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately."[44] Plaintiffs' ability (or inability) to prove exfiltration does not bear on their stated theory of the case presented in their Motion. But even if it did, the spoliated evidence would not demonstrate exfiltration. The loss of A23567-D and the DLP logs are at most minimally prejudicial to Plaintiffs.

Conclusion

Premera asks that Plaintiff's Motion for Sanctions be denied pursuant to Rule 37(e), and that Plaintiff's Motion for Sanctions, to the extent it relies upon the Court's inherent authority, also be denied. If Plaintiffs wish to recreate the data related to DLP

[43] *Id.* at 3.

[44] *See, e.g.*, Sherer Decl. Ex. 15, Notification Letter to Elizabeth Black (PBC00009500).

policy violations through Vontu Alert mail, Premera is willing to collect and produce such data if so ordered by the Court.

Dated: October 9, 2018

Daniel R. Warren
David A. Carney
dwarren@bakerlaw.com
dcarney@bakerlaw.com
BAKER & HOSTETLER LLP
127 Public Square, Suite 2000
Cleveland, OH 44114
Telephone: 216.621.0200

Paul G. Karlsgodt
pkarlsgodt@bakerlaw.com
BAKER & HOSTETLER LLP
1801 California Street, Suite 4400
Denver, CO 80202
Telephone: 303.861.0600

BAKER & HOSTETLER LLP

/s/ James A. Sherer

James A. Sherer
jsherer@bakerlaw.com
BAKER & HOSTETLER LLP
45 Rockefeller Plaza
New York, NY 10111
Telephone: 212.589.4200

Darin M. Sands
SandsD@LanePowell.com
LANE POWELL PC
601 SW Second Ave, Suite 2100
Portland, OR 97204-3158
Telephone: 503.778.2117

Attorneys for Defendant Premera Blue Cross

CERTIFICATE OF SERVICE

I certify that on the 9th day of October, 2018 the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ James A. Sherer
One of the Attorneys for Defendant Premera Blue Cross